ROYAL BOROUGH OF WINDSOR AND MAIDENHEAD

www.rbwm.gov.uk Royal Borough of Windsor & Maidenhead

SECURITY POLICY

USE OF MOBILE PHONES

Introduction and Policy Aim

This policy covers the deployment and use of mobile telephones and Internet smartphones. It includes the rules needed for their safe and secure use. The term 'mobile phone' refers either to a basic mobile phone, or to an Internet smartphone.

Policy Statement

The council may provide mobile phones for use on council business. These mobile phones (however obtained) are subject to this policy.

Council mobile phones must be authorised by a council Head of Service or higher grade.

When a council mobile phone is used, the person using it will be deemed to have accepted the rules and conditions in this policy. That person will be responsible for keeping the phone, and data stored on it, secure.

Not covered by this Policy

The use of any fixed location/desktop telephones used for council business.

Those Affected by the Policy

This policy applies to Councillors, employees of the council, contractors, agency staff, and others working in a similar capacity. It also applies to volunteers and partner organisations, and individuals who do work for the council.

It does not cover work done by external consultants who independently use their own IT technology and information assets. Their UK Data Protection Act and information protection obligations must be stated in their contract for council work.

Roles and Responsibilities

1. Councillors, employees and others – will have confirmed their acceptance of this policy by using a mobile phone to conduct council business.
2. Council Directors, Heads of Service, Service Leads and Managers – the council manager responsible for the work being done must ensure those working under their supervision have read and agreed to this policy.
3. The Council IT Service – is responsible for:
   (a) ensuring that all mobile phones are set up securely before being issued
   (b) maintaining an accurate, up to date asset register of mobile phones.
4. Information Governance Team – is responsible for defining & communicating mobile phone security rules and guidance, and for compliance monitoring.

Policy Compliance

Compliance with this policy is required so that the council can meet its operational requirements and Data Protection Act obligations. If you are found to have breached this policy by not complying with its rules and responsibilities you may be subject to the council's disciplinary procedure or other action.
If you are suspected of breaking the Law, you may be subject to prosecution.
If you do not understand the implications of this policy, or how it may apply to you,

seek advice from your council manager, the IT Service, or the Information Governance Team.

Applying the Policy - Equipment

Rule 1 Use of council mobile phones must be authorised in writing by a council Head of Service or higher grade.

Rule 2 A Portable Electronic Device Security Declaration must be signed before any mobile phone and related equipment is issued by the IT Service.

Rule 3 An Information Asset Register containing the names and phone details of council mobile phone users must be maintained by the IT Service.

Mobile Phone and SIM Card Return or Transfer

Rule 4 When a phone is transferred to a new user, the recipient must sign the Portable Electronic Device Security Declaration before using the phone.

Rule 5 All SIM cards must be returned to the IT Service when no longer used. It is the phone user's responsibility to delete personal information from the SIM card before its return.

Rule 6 Phone handsets that are no longer required must be returned to the IT Service for re-issue, secure destruction or recycling. It is the user's responsibility to delete all information stored on the phone itself before it is returned.

Applying the Policy

The council officer issued with a mobile phone is responsible for its security, and must take all reasonable care to avoid loss, damage or misuse.

Loss or Theft of Mobile Phones

When a mobile phone is lost or stolen, the council phone user must do the following as soon as possible:

Rule 7 Get the phone SIM blocked by the council's telecommunications provider who should offer a 24x7 telephone Help Desk facility. The IT Service can also arrange for the SIM card to be blocked.

Rule 8 Contact the police, report the loss or theft, and obtain a crime reference number. Send the police reference number to the council's Insurance and Risk Management Team.

Rule 9 Report the loss to the council manager responsible and submit a Security Incident Report as soon as possible. Phone data loss questions will then be sent to the person reporting the phone loss or theft. The answers to the questions must be sent to security@rwm.gov.uk.

Protecting the Phone Against Unauthorised Access

Mobile phones may carry business related emails and attachments of a personal or sensitive nature. They may also carry personal phone numbers.

To prevent security breaches it is the phone user's responsibility to protect their phone from being accessed by strangers or unauthorised people.

Some of the security measures below may be applied centrally by the IT Service for Internet-enabled smartphones. The phone user should contact the IT Service Desk with any questions about security settings.

Rule 10 A PIN number or password must be set up to protect the phone SIM Card.

Information on how to set the PIN or password for a specific model of mobile phone will be provided in the handset instructions or on the manufacturer's website.

Rule 11 PIN numbers and passwords must not be disclosed or told to others.

Do not use obvious PIN numbers, e.g. 0000, 1111, 1234, 9999, 2014, your own birth date. Make each PIN digit different, and use a number that is personal to you and easy to remember.

Set handset locks or timeouts

It is good security practice to make your mobile phone lock itself after several minutes if not used, or to lock itself when put into a protective case.

Rule 12 If a council phone has a GPS tracking facility it must be left switched on. This may allow it to be located using the GPS signal.

Any instructions communicated by the IT Service on security measures such as remote disablement following loss must be followed.

Use of Mobile Phones Abroad

Security risks are significantly higher if mobile phone services are used outside the United Kingdom. Public Internet connections accessed from outside the UK are not secure, and must not be used to access sensitive personal data. Emails containing sensitive or personal data must not be sent or accessed outside the UK.

Rule 13 A Director or Head of Service's written authorisation must be obtained before taking a mobile phone out of the UK.

Rule 14 When using a council mobile phone abroad, follow the advice provided on how to avoid potentially high costs of roaming and downloading.

Legal Obligations

UK Data Protection Act

Related Policies, Procedures and Guidance

Electronic Information Asset Management Policy
Information Commissioner's Guidance 'Safer Smartphones'
Information Handling Security Policy
Remote Working Security Policy